WHAT IS CLAIMED IS:

1. A group formation/management system, comprising:

one or more registered member devices operable to hold common secret information unique to a group;

a new member device operable to transmit a request for registration to the group, and to receive and hold the common secret information; and

a group management device operable to receive the registration request from the new member device, and when a registered number of member devices is less than a maximum number of member devices registerable in the group, to register the new member device and output the common secret information to the new member device.

2. A group formation/management system, comprising:

a member device operable to transmit a request for registration to a group, and to receive and hold common secret information unique to the group; and

a group management device operable to receive the registration request from the member device, and when a registered number of member devices is less than a maximum number of member devices registerable in the group, to register the member device and output the common secret information to the member device, wherein

in an initial state, the group has no member devices registered therein.

3. A group management device that manages a group, comprising:

a reception unit operable to receive from a member device, a request for registration to the group;

a judging unit operable, if the member device is authenticated as being a legitimate device, to judge whether a registered number of member devices is less than a maximum number of member devices registerable in the group, and to register the member device when judged in the affirmative; and

a communication unit operable, when the judging unit judges in the affirmative, to output to the member device, common secret information unique to the group.

4. The group management device of claim 3, wherein

the judging unit includes:

an authentication subunit operable to hold a second initial value, and to authenticate the member device, using the second initial value and a first initial value held by the member device; and

a device-number judging subunit operable, when

authentication is successful, to judge whether the registered number is less than the maximum number,

the common secret information outputted by the communication unit shows "registered in the group", and

the member device receives and holds the outputted common secret information, and deactivates the first initial value.

5. The group management device of claim 4, wherein

the first and second initial values show "unregistered in the group".

6. The group management device of claim 4, wherein

the first and second initial values show "unregistered in any group".

7. The group management device of claim 3, further comprising:

a generating unit operable to generate the common secret information, wherein

the communication unit outputs the generated common secret information to the member device.

8. The group management device of claim 3, wherein

the common secret information is generated by a management device outside of the group,

the judging unit receives the common secret information from the out-group management device, and

the communication unit outputs the received common secret information to the member device.

9. The group management device of claim 3, wherein

the reception unit, on receipt of the registration request, notifies the receipt to a management device outside of the group,

the out-group management device judges whether the registered number is less than the maximum number,

the judging unit, instead of judging whether the registered number is less than the maximum number, receives a judgment result from the out-group management device, and

the communication unit outputs the common secret information to the member device, when the judgment result shows that the registered number is less than the maximum number.

10. The group management device of claim 3, wherein

the maximum number is formed from a first maximum number and a second maximum number, and

the judging unit judges whether the registered number is less than one of the first maximum number and the second maximum number, and registers the member device when judged in the affirmative.

11. The group management device of claim 10, wherein

the first maximum number is the number of member devices, out of the maximum number, connectable to the group management device, and the second maximum number is the number of member devices, out of the maximum number, not connectable to the group management device, and

the judging unit judges, (i) when the member device is connectable to the group management device, whether the registered number of connectable member devices is less than the first maximum number, and (ii) when the member device is not connectable to the group management device, whether the registered number of non-connectable member devices is less than the second maximum number.

12. The group management device of claim 3, wherein

the communication unit outputs to another group management device, a request inquiring whether the member device is registerable in the other group management device,

the other group management device receives the inquiry

request, judges whether a registered number of member devices is less than a maximum number of member devices registerable with the other group management device, and when judged in the affirmative, registers the member device and outputs the common secret information to the group management device, and

the communication unit, on receipt of the common secret information from the other group management device, outputs the received common secret information to the member device.

13. The group management device of claim 3, wherein

the judging unit functions to resist invalid access from outside, and

the maximum number and the common secret information are stored in an area that is unreadable/unwritable from outside.

14. The group management device of claim 13, wherein

the judging unit is included in a portable module that is mountable in the group management device.

15. The group management device of claim 3, wherein

the judging unit stores a remaining number obtained by subtracting the registered number from the maximum number,

and on receipt by the reception unit of the registration request, judges whether the remaining number is "0", and when judged that the remaining number is not "0", the communication unit outputs the common secret information to the member device and the judging unit subtracts "1" from the remaining number.

16. The group management device of claim 3, wherein

the reception unit, after the outputting of the common secret information, receives from the member device, a request for withdrawal from the group,

the communication unit, on receipt by the reception unit of the withdrawal request, outputs to the member device, a notification indicating to delete the common secret information,

the reception unit receives from the member device, a notification showing that deletion of the common secret information has been completed, and

the judging unit, on receipt by the reception unit of the deletion-completed notification, reduces the registered number.

17. The group management device of claim 3, wherein

the judging unit, when judged that the registered

number is less than the maximum number, issues information showing a valid period during which use of the common secret information is permitted in the member device, increases the registered number, monitors the elapse of the valid period, and reduces the registered number when the valid period ends, and

the communication unit outputs the issued information to the member device.

18. The group management device of claim 3, wherein

the judging unit receives from a management device outside of the group, a number of member devices registerable in the group, pays an accounting fee in accordance with the received number, and sets the received number as the maximum number.

19. The group management device of claim 3, wherein

the judging unit newly acquires from a management device outside of the group, a number of member devices registerable in the group, pays an accounting fee in accordance with the acquired number, and adds the acquired number to the maximum number to obtain a new maximum number.

20. The group management device of claim 3, wherein

the reception unit, after the outputting of the common secret information, receives a communication request from the member device,

the judging unit authenticates the member device using the common secret information and common secret information held by the member device, and

the communication unit communicates with the member device when authentication is successful.

21. The group management device of claim 3, further comprising:

a content storage unit operable to store therein a content key and an encrypted content encrypted using the content key; and

an encryption unit operable to encrypt the content key using a key generated based on the common secret information, to generate an encrypted content key, wherein

the communication unit outputs the encrypted content and the encrypted content key to the member device.

22. The group management device of claim 21, wherein

the judging unit authenticates the member device using the common secret information and common secret information held by the member device, and shares a session key with the

member device, using the common secret information, and

the encryption unit, when authentication is successful, encrypts the content key using the shared session key.

23. The group management device of claim 3, wherein

the communication unit stores therein the common secret information, newly receives a different piece of common secret information, overwrites the stored common secret information with the newly received common secret information, and outputs, regularly or irregularly, the newly received common secret information to the member device.

24. The group management device of claim 3, further comprising:

a content storage unit operable to store therein a content key and an encrypted content encrypted using the content key;

an encryption unit operable to encrypt the content key using a key generated based on the common secret information, to generate an encrypted content key; and

a writing unit operable to write the encrypted content and the encrypted content key to a portable recordable medium.

25. The group management device of claim 24, wherein

the received registration request includes an identifier identifying the member device, and

the encryption unit encrypts the content key using a key generated based on the common secret information and the identifier, to generate the encrypted content key.

26. The group management device of claim 24,

the encryption unit encrypts the content key using a key generated based on the common secret information and an identifier unique to the portable recordable medium.

27. The group management device of claim 3, further including:

a holding unit operable to hold, in correspondence with identifiers that each identify a different group, (i) common secret information unique to the group and (ii) a maximum number of member devices registerable in the group, wherein

the received registration request includes one of the identifiers,

the judging unit, on receipt by the reception unit of the registration request, judges whether the number of member devices registered in a group identified by the identifier is less than a maximum number corresponding to the identifier,

and when judged in the affirmative, registers the member device in the group and selects common secret information corresponding to the identifier, and

the communication unit outputs the selected common secret information to the member device.

28. The group management device of claim 3, wherein

the received registration request requests the registration of a predetermined number of other member devices,

the judging unit judges whether an aggregate number obtained by adding the predetermined number to the registered number is less than the maximum number, and when judged in the affirmative, generates a permission right permitting a copying of the common secret information to the predetermined number of member devices, and

the permission right is attached to the outputted common secret information.

29. The group management device of claim 3, wherein

the received registration request includes a first identifier unique to the member device,

the judging unit stores therein the first identifier,

the reception unit, after the outputting of the common

secret information, receives a second identifier unique to the member device,

the judging unit judges whether the second identifier matches the first identifier, and

the communication unit, when judged that the first and second identifiers match, again outputs the common secret information to the member device.

30. The group management device of claim 3, wherein

when the group management device is determined to be a new group management device for managing a new group formed by combining groups managed by a plurality of group management devices, the communication unit outputs to member devices registered in the groups, new common secret information unique to the new group, and

when one of the other group management devices is determined to be the new group management device, the group management device further comprises:

a receiving unit operable to receive the new common secret information from the other group management device; and

a holding unit operable to hold the received new common secret information.

31. The group management device of claim 30, wherein

the communication unit determines in conjunction with the other group management devices, one of the group management devices to be the new group management device.

32. The group management device of claim 31, wherein

the holding unit stores therein a priority level of the group management device, and

the communication unit determines, out of the stored priority level and priority levels of the other group management devices, the group management device having the highest priority level to be the new group management device.

33. The group management device of claim 30, wherein

each member device registered in the groups managed by the group management device and the other group management devices has a priority level, and

when the group management device is determined to be the new group management device, the reception unit acquires the priority levels of the member devices,

the group management device further comprises a selecting unit operable to select, in order from highest to lowest of the acquired priority levels, member devices for registration in the new group, the selected number of member

devices being less than or equal to a maximum number of member devices registerable in the new group, and

the communication unit outputs the new common secret information to the selected member devices.

34. The group management device of claim 3, further comprising:

a determining unit operable, after the outputting of the common secret information, to determine a member device registered in the group to be another group management device; and

a dividing unit operable to divide member devices registered in the group into member devices to be registered in a group managed by the group management device and member devices to be registered in another group managed by the other group management device, and

the communication unit outputs, after the dividing by the dividing unit, a different piece of common secret information to the member devices to be registered in the group managed by the group management device.

35. A member device that uses a content after registering in a group managed by a group management device, comprising:

a requesting unit operable to request the group

management device for registration to the group;

a receiving unit operable to be authenticated by the group management device, and to receive from the group management device, common secret information unique to the group; and

a holding unit operable to hold the received common secret information.

36. The member device of claim 35, wherein

the holding unit holds a first initial value,

the receiving unit is authenticated by the group management device using the first initial value, and receives the common secret information from the group management device when authentication is successful, and

the holding unit deactivates the first initial value and holds the received common secret information.

37. The member device of claim 36, wherein

the first initial value shows "unregistered in the group".

38. The member device of claim 36, wherein

the first initial value shows "unregistered in any group".

39. The member device of claim 36, wherein

the holding unit overwrites the first initial value with the common secret information.

40. The member device of claim 36, further comprising:

a communication unit operable, after the holding of the common secret information, to output the common secret information to another member device; and

a deletion unit operable to delete the held common secret information after the outputting by the communication unit, wherein

the holding unit reactivates the first initial value after the deleting by the deletion unit.

41. The member device of claim 36, wherein

the requesting unit requests the group management device for withdrawal from the group,

the receiving unit receives from the group management device, a notification indicating to delete the common secret information, and

the holding unit deletes the held common secret information and reactivates the first initial value.

42. The member device of claim 35, wherein

the receiving unit, after the holding of the common secret information, newly receives a different piece of common secret information from the group management device, and

the holding unit overwrites the held common secret information with the newly received common secret information.

43. The member device of claim 35, wherein

the requesting unit requests the group management device for delivery of the content,

the receiving unit receives from the group management device, an encrypted content generated by encrypting the content using a content key, and an encrypted content key generated by encrypting the content key using an encryption key generated based on the common secret information, and

the member device further comprises a decryption unit operable to generate a decryption key the same as the encryption key, based on the common secret information, to decrypt the encrypted content key using the decryption key to obtain a content key, and to decrypt the encrypted content using the content key to obtain a content.

44. The member device of claim 35, wherein

the holding unit includes a storage subunit that is unreadable/unwritable from outside, and

the storage subunit stores therein the received common secret information.

45. The member device of claim 44, wherein

the storage subunit is a recording medium mountable in the member device.

46. The member device of claim 35, further comprising:

an authentication unit operable, after the holding of the common secret information, and when the member device communicates with another member device, to authenticate the other member device using the held common secret information and common secret information held by the other member device.

47. The member device of claim 35, further comprising:

a communication unit operable, after the holding of the common secret information, to output the common secret information to another member device; and

a deletion unit operable to delete the held common secret information after the outputting by the communication unit.

48. The member device of claim 35, wherein:

the requesting unit requests the group management device for withdrawal from the group,

the receiving unit receives from the group management device, a notification indicating to delete the common secret information, and

the holding unit, on acquisition of the deletion notification by the receiving unit, deletes the held common secret information.

49. The member device of claim 35, wherein

the received common secret information includes information showing a valid period during which use of the common secret information is permitted in the member device, and

the holding unit monitors an elapse of the valid period and deletes the common secret information when the valid period ends.

50. The member device of claim 35, wherein

the requesting, receiving and holding units are included in a portable module that is mountable in the member device and the group management device, and

the receiving unit receives the common secret

information from the group management device, when the portable module is mounted in the group management device.

51. The member device of claim 50, wherein

the receiving unit receives from the group management device, an encrypted content encrypted using a content key, and an encrypted content key generated by encrypting the content key using an encryption key generated based on the common secret information, and

the member device further comprises:

a decryption unit operable to read the common secret information from the mounted portable module, generate a decryption key the same as the encryption key, based on the read common secret information, decrypt the encrypted content key using the decryption key to obtain a content key, and decrypt the encrypted content using the content key to obtain a content.

52. The member device of claim 50, wherein

the portable module further includes:

a notifying unit operable, when the portable module is mounted in the member device, to notify the held common secret information to the member device; and

a management unit operable, after the notifying of the

held common secret information, to prohibit the notifying unit from again notifying the held common secret information to the member device, and

the member device further comprises a storage unit operable to receive and store therein the common secret information notified from the portable module.

53. The member device of claim 35, wherein

the holding unit holds a maximum holdable number, which is the number of pieces of common secret information holdable by the holding unit, and

the requesting unit requests the group management device for registration to the group when the number of pieces of held common secret information is less than the maximum holdable number.

54. The member device of claim 53, wherein

the holding unit holds identifiers that each identify a different group,

the registration request includes one of the identifiers, and

the holding unit holds the received common secret information in correspondence with the identifier included in the registration request.

55. The member device of claim 35, wherein

the requesting unit requests the group management device for registration of a predetermined number of other member devices,

the received common secret information has attached a permission right permitting a copying of the common secret information to the predetermined number of member devices,

the member device further comprises a communication unit operable to output the common secret information to another member device, and

the holding unit reduces the number of copies permitted by the permission right by "1" when the common secret information is outputted by the communication unit.

56. The member device of claim 55, wherein

the holding unit holds an identifier unique to the member device,

the communication unit acquires from the other member device, an identifier unique to the other member device, and

the requesting unit transmits the held and acquired identifiers to the group management device.

57. The member device of claim 35, wherein

the holding unit holds an identifier unique to the

member device,

the registration request includes the identifier,

the holding unit, on receipt of a power-OFF instruction, deletes the held common secret information and sets power off, and

on receipt of a power-ON instruction, the requesting unit again transmits the identifier to the group management device, and the receiving unit again receives the common secret information from group management device.

58. The member device of claim 35, wherein

the holding unit holds an identifier unique to the member device,

the registration request includes the identifier,

the holding unit, when communication with the group management device is interrupted, deletes the held common secret information, and

when communication with the group management device is reestablished, the requesting unit again transmits the identifier to the group management device, and the receiving unit again receives the common secret information from group management device.

59. The member device of claim 35, wherein

the receiving unit, after the holding of the common secret information, newly receives a different piece of common secret information from one of the group management device and another group management device, and

the holding unit deactivates the held common secret information and holds the newly received common secret information.

60. The member device of claim 35, further comprising:

a dividing unit operable, after the holding of the common secret information, and when the member device is determined by the group management device to be another group management device, to divide member devices registered in the group into member devices to be registered in a group managed by the group management device and member devices to be registered in another group managed by the other group management device; and

a communication unit operable to output to the member devices to be registered in the other group, common secret information unique to the other group.

61. The member device of claim 60, wherein

the member devices registered in the group each have a priority level,

the receiving unit acquires the priority levels of the other member devices, and

the dividing unit conducts the dividing based on the acquired priority levels.

62. A registration device that registers a member device in a group managed by a group management device, comprising:

a holding unit operable to receive from the group management device and hold, common secret information unique to the group; and

a notifying unit operable, when the registration device is connected to the member device, to notify the common secret information to the member device.

63. The registration device of claim 62, further comprising:

a management unit operable, after the notifying of the common secret information, to prohibit the notifying unit from again notifying the common secret information to the member device.

64. The registration device of claim 62, further comprising:

a reception unit operable to receive from the member device, a request for acquisition of the common secret information, wherein

the notifying unit notifies the common secret information to the member device when the acquisition request is received by the reception unit.

65. A member device that uses a content after registering in a group managed by a group management device, comprising:

a selecting unit operable to select one of a plurality of group management devices based a preset criterion;

a requesting unit operable to request the selected group management device for registration to a group;

a receiving unit operable to receive, from the selected group management device, common secret information unique to the group; and

a holding unit operable to hold the received common secret information, wherein

the preset criterion is, with respect to each group management device, one of (i) a distance from the member device, (ii) a communication time with the member device, (iii) a processing capacity, and (iv) a processing state.

66. An authentication method used in a group management device that manages a group, comprising the steps of:

receiving a request from a member device;

authenticating whether the member device is a

legitimate device, using common secret information unique to the group and common secret information held by the member device; and

judging the member device to be registered in the group when authentication is successful.

67. A computer program used in a group management device that manages a group, comprising the steps of:

receiving a request from a member device;

authenticating whether the member device is a legitimate device, using common secret information unique to the group and common secret information held by the member device; and

judging the member device to be registered in the group when authentication is successful.

68. A recording medium storing a computer program used in a group management device that manages a group, the computer program comprising the steps of:

receiving a request from a member device;

authenticating whether the member device is a legitimate device, using common secret information unique to the group and common secret information held by the member device; and

judging the member device to be registered in the group when authentication is successful.